A note on splitting fields for twisted group algebras of finite groups over a number field

Hans Opolka

Technische Universität Braunschweig

Institut für Analysis und Algebra

Universitätsplatz 2

D-38106 Braunschweig

e-mail: h.opolka@tu-bs.de

Abstract The main purpose of this note is to provide a splitting field for a twisted group algebra of a finite group over a number field which depends only on the exponent of the finite group and on certain prescibed arithmetic conditions for the underlying cocycle.

Mathematics subject classification 2020: 16K99, 20C05, 20C25. 12F05, 11R27

Key words and phrases: Twisted group algebras, splitting fields, number fields, units

1. A splitting field for a twisted group algebra constructed from the underlying cocycle

Let k be a field of characteristic 0, let C be an algebraically closed extension field of k, let G be a finite group, let $f: G \times G \to k^*$ be a central 2-cocycle and denote by (k, G, f) the twisted group algebra of G over k with respect to f, i.e. (k, G, f) is the k-vector space with basis $(e_x : x \in G)$, and the ring multiplication in (k, G, f) is obtained by k-linear extension of the rule

$$e_x e_y = f(x, y) e_{xy}\,, \quad x, y \in G\,.$$

For basic concepts and results on twisted group algebras we refer to [Y], §4. Especially we use the well kown fact that (k, G, f) is semisimple and that the representations of (k, G, f) over k correspond bijectively to the k-f-

https://doi.org/10.24355/dbbs.084-202104161401-0

representations of G, i.e. to the mappings $T: G \to GL(V)$, where $GL(V)$ is the group of k-automorphisms of a finite dimensional k-vector space V, such that

$$T(x)T(y) = f(x,y)T(xy) \text{ for all } x, y \in G.$$

For general background information and basic results on algebras we refer to [D].

This note makes use of the splitting field of (k, G, f) which was constructed in [O1]. We recall its construction: For every $x \epsilon G$ define

$$a_f(x) \coloneqq \prod_{i=1}^{m(x)} f(x, x^i), \text{ where } m(x) \coloneqq order\ of\ x\ ,$$

and let $L_f \subset C$ denote a splitting field for all polynomials

$$X^{m(x)} - a_f(x), \quad x \in G\ .$$

(1.1) **Theorem** *L_f is a splitting field for (k, G, f)*

For a proof see [O1].

We use the following notation: W_k is the group of roots of unity in k. W_m is the group of roots of unity in C of order dividing m. ξ_m is a primitive root of unity of order m in C.

(1.2) Remarks and examples (a) Another method for constructing splitting fields of twisted group algebras is discussed in [O2]. It makes use of the concept of *lifting field*; see especially [O2], (1.2), p. 3.

(b) If k contains a primitive root of unity of order $\exp(G)$ then L_f/k is an abelian extension. This case occurs for instance in the context of symbol algebras. Namely, let G be a finite abelian group, let k be a field of characteristic 0 and let $f: G \times G \to k^*$ be a central 2-cocycle such that the associated symplectic pairing which is defined e.g. in [Y], §2, i.e.

$$\omega_f: G \times G \to k^*\ , \quad \omega_f(x,y) \coloneqq \frac{f(x,y)}{f(y,x)}\ ,\ x, y \in G,$$

is nondegenerate. Then k contains a primitive root of unity of order $\exp(G)$. It follows almost immediately from the definitions and is well known that every symbol algebra, as defined and discussed e.g. in [MN], § 15, is

https://doi.org/10.24355/dbbs.084-202104161401-0

isomorphic to (k, G, f) where $G \cong C(m) \times C(m)$ is a direct product of isomorphic cyclic groups of order m for some m and f is a central 2-cocycle such that ω_f is nondegenerate. Hence in this case k contains a primitive root of unity of order $m = \exp(G)$.

(c) Represent an element (f) in the Schur multiplier of a finite group G by a central 2-cocycle $f: G \times G \to W_m$, where m is the order of (f), and let $k = \mathbb{Q}(\xi_m)$. According to [AK] the exponent of the Schur multplier of a finite group G divides the number $|G|/\exp(G)$. This implies that the field L_f is contained in the cyclotomic field $\mathbb{Q}(\xi_{|G|})$. Therefore (1.1) yields part of a result of W. F. Reynolds [RE], see Theorem on p. 191 and its proof; in particular it shows that every projective representation of G over $\mathbb{C}$ can be realized over $\mathbb{Q}(\xi_{|G|})$.

2. A splitting field for twisted group algebras over a number field with prescribed arithmetic conditions for the underlying cocycle

Let k be a number field with ring of integers $R = R_k$, let G be a finite group of exponent e, let S be a finite set of places of k which contains all infinite places of k and all places of k which divide e, let R_S denote the ring of S-integers of k and let R_S^* be its group of units. The generalized Dirichlet unit theorem shows that

$$R_S^* \cong W_k \times \mathbb{Z}^{s-1} \tag{2.1}$$

where s is the number of elements of S, comp. e.g. [L1], p. 105. As in [O2], p. 8, line 1, a central 2-cocycle $f: G \times G \to k^*$ is said to be *unramified outside* S if its cohomology class $(f) \in H^2(G, k^*)$ is contained in the image of the homomorphism

$$H^2(G, R_S^*) \to H^2(G, k^*) \tag{2.2}$$

which is induced by the embedding $R_S^* \hookrightarrow k^*$. Denote this image by $H^2(G, k^*)_S$. As was shown in [O2], section 2, p. 7, the group $H^2(G, R_S^*)$ - and therefore also the group $H^2(G, k^*)_S$ - is finite. Of course every central 2-cocycle $f: G \times G \to k^*$ is unramified outside some suitable set of places S as above.

https://doi.org/10.24355/dbbs.084-202104161401-0

(2.3) **Theorem** *Let k be a number field, let e be a positive integer and let S be a finite set of places of k which contains all infinite places of k and all places of k which divide e. Let $L = K(S,e) \subset C$ be the splitting field of all polynomials $X^e - a$, where $a \in R_S^*$ runs through a full set Q of representatives of the finite group R_S^*/R_S^{*e}. Then $L = K(S,e)$ is a splitting field for all twisted group algebras (k,G,f), where G is a finite group of exponent e and where the central 2-cocycle f is unramified outside S.*

Proof: Since cohomologous cocycles yield isomorphic twisted group algebras we may and do assume that in (k,G,f) all values of f belong to R_S^*. It is then sufficient to show that the splitting field L_f of (k,G,f) which is defined in (1.1) is contained in L. But this follows by expressing each

$$a_f(x) = \prod_{i=1}^{m(x)} f(x,x^i)\,, \quad x \in G,$$

as

$$a_f(x) = a \cdot b^e\,,\ a \in Q,\ b \in R_S^*\,,$$

which shows that all e-th roots of $a_f(x)$ in C are contained in L. It implies that all $m(x)$-th roots of $a_f(x)$ are contained in L. So L contains L_f.

(2.4) **Remarks and examples** (a) If in (2.3) the field k contains a primititive root of unity of order e then the extension $K(S,e)/k$ is abelian. For example, for $k = \mathbb{Q}$ this assumption means $e = 2$, i.e. the finite groups G are elementary abelian of exponent 2, and if the finite set of places S of $\mathbb{Q}$ consists of the infinite place and the places corresponding to prime numbers $2, p_1, \dots, p_r$, then

$$R_S^* = < -1, 2, p_1, \dots, p_r > \text{ and } K(S,2) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}).$$

(b) E. Artin's construction of the Clifford algebra $C(q)$ of a nondegenerate quadratic form q over a field k of characteristic $\neq 2$ as a twisted group algebra (k,G,f) of a finite elementary abelian group G of exponent 2 as given in [A], chapter V, section 4, especially p. 186, line 26, applied in the situation where k is a number field, shows that f is unramified outside S, where S is such that the diagonal coefficients of q are S-units, and therefore by (2.3) the field $K(S,2)$ is a splitting field for $C(q)$ for all such nondegenerate quadratic forms q over k - which of course is obvious and well known.

https://doi.org/10.24355/dbbs.084-202104161401-0

(c) We discuss an example which makes use of basic facts from the theory of elliptic curves over number fields; for the latter we refer to [SI], Chapter VIII, and to [T], especially section 3. A related construction, which aims at Galois representations, is contained in e.g. [J], section 4.3. Let m be an integer >1, let k be a number field with algebraic closure $\bar{k}$, assume that k contains the group of m-th roots of unity $W_m \leq \bar{k}$. Let S be a finite set of places of k which contains all infinite places of k, all places which divide m and large enough such that the ring R_S of S-integers of k is a principal ideal ring. Let k_S/k denote the maximal extension which is unramified outside S and let G_S denote the Galois group of this extension. Let E be an elliptic curve defined over k. Assume that S contains all places of k where E has bad reduction. Then, as remarked in [T], section 3, $E(k_S)$ is divisible by m and the multiplication by m map $E(k_S) \overset{m}{\to} E(k_S)$ gives an exact sequence of G_S-groups

$$0 \to E_m \to E(k_S) \overset{m}{\to} E(k_S) \to 0 \tag{1}$$

where E_m is the group of m-torsion points of E over $\bar{k}$; as an abstract group E_m is isomorphic to a direct product of isomorphic cyclic groups of order m: $E_m \cong C(m) \times C(m)$. Assume furthermore that k contains the coordinates of all elements of E_m. Then $H^1(G_S, E_m) = Hom(G_S, E_m)$, and the exact cohomology sequence applied to (1) yields the exact sequence

$$0 \to E(k)/mE(k) \overset{\Delta}{\to} Hom(G_S, E_m) \to H^1(G_S, E)_m \to 0\,. \tag{2}$$

Put $G \coloneqq C(m) \times C(m)$. We will construct a central 2-cocycle $f\colon G \times G \to R_S^*$. Let $\omega\colon G \times G \to W_m$ be the Weil Pairing, see e.g. [SI], Chapter III, §8, and denote by $f_\omega\colon G \times G \to W_m$ the corresponding pairing – and therefore cocycle - constructed in the proof of [Y], 2.3, Theorem 2.2. So ω satisfies

$$\omega(x, y) = f_\omega(x, y)/f_\omega(y, x) \text{ for all } x, y \in G.$$

Assume that there is a surjective $\varphi \in Hom(G_S, E_m)$ and denote by K the corresponding kernel field. So K/k is a Kummer extension of exponent m which is unramified outside S and its Galois group is isomorphis to G. As is well known from Kummer theory over number fields there are elements $a, b \in R_S^*$ such that $K = k\left(\sqrt[m]{a}, \sqrt[m]{b}\right)$. Assume that x, y are generators of G, i.e. $G = \langle x\rangle \times \langle y\rangle$. Define a central 2-cocycle $f_a\colon \langle x\rangle \times \langle x\rangle \to R_S^*$ by

$$f_a\left(x^i, x^j\right) \coloneqq 1,\ if\ i + j < m,\ and\ f_a\left(x^i, x^j\right) \coloneqq a,\ if\ i + j \geq m\,,$$

and in the same way a central 2-cocycle $f_b\colon \langle y\rangle \times \langle y\rangle \to R_S^*$. Then

$$f_a \times f_b\colon G \times G \to R_S^*$$

https://doi.org/10.24355/dbbs.084-202104161401-0

is a symmetric central 2-cocycle. This construction is well known from group cohomology and occurs in a similar context in the description of cyclic algebras, see e.g. [D], II, §5, p. 65. Finally the sought-for central 2-cocycle $f: G \times G \to k^*$ is defined as

$$f: G \times G \xrightarrow{(f_a \times f_b)\cdot f_\omega} R_S^* \hookrightarrow k^* .$$

It follows from (2.3) that the field $K(S, m)$ is a splitting field for the twisted group algebra (k, G, f). The question arises whether there are examples where a surjective $\varphi \in Hom(G_S, E_m)$ can be obtained from a rational point, i.e. where there exists $P \in E(k)$ such that

$$\varphi = \Delta\big(P \bmod mE(k)\big),$$

Δ being the map occuring in the above exact sequence (2). This question can be studied by applying Kummer theory for elliptic curves as presented e.g. in [L2], Chapter V. Compare also related questions and investigations in the context of Galois representations in [J], sections 4.2, 4,3, 4.4 .

References

[AK] J.L. Alperin, T.-N. Kuo: The exponent and the projective representations of a finite group, Illininois Journal of Mathematics, 11, 1967, 410-413

[A] E. Artin: *Geometric Algebra*, Interscience Publishers, New York, 1957

[D] M. Deuring: *Algebren*, Zweite, korrigierte Auflage, Springer Verlag, Berlin, 196

[J] F. Jonas: *Einbettungsprobleme und Galoisdarstellungen mit beschränkter Verzweigung*, Dissertation, Universität Göttingen, 1991

[L1] S. Lang: *Algebraic Number Theory*, second edition, Springer Verlag, New York, 1994

[L2] S. Lang: *Elliptic Curves Diophantine Analysis*, Springer Verlag, Berlin 1978

[MN] J. Milnor: *Introduction To Algebraic K-Theory*, Annals of Mathematics Studies, Princeton University Press, Number 72, Princeton, New Jersey, 1971

[O 1] H. Opolka: Cocycles, radicals and splitting fields of twisted group algebras, https://doi.org/10.24355/dbbs.084-201810301515-0

https://doi.org/10.24355/dbbs.084-202104161401-0

[O 2] H. Opolka: Lifting problems for projective representations of finite groups over number fields, https://doi.org/10.24355/dbbs.084-202009251215-0

[RE] W.F. Reynolds: Projective representations of finite groups in cyclotomic fields, Illinois Journal of Mathematics, 9, 1965, 191-198

[SI] J. H. Silverman: *The Arithmetic of Elliptic Curves*, Springer Verlag, New York, 1986

[T] J. Tate: *Galois Cohomology*, Arithmetic algebraic geometry (Park City, UT, 1999) IAS/Park City Mathematics Series, vol. 9, American Math. Soc., Providence, RI, 2001, pp. 465-479

[Y] K. Yamazaki: On projective representations and ring extensions of finite groups, Journal of the Faculty of Science of the University of Tokyo, Section I, 10, 1964, 147-195